UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/869,435	06/28/2001	Louis Goubin	T2146-907343	2705

181 7590 10/06/2004

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 10/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/869,435	GOUBIN, LOUIS	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-7 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-7 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 6/28/2004.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-7 have been examined and are rejected under 35 U.S.C. 102(e).

Claim Rejections - *35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-7 are rejected under 35 U.S.C. 102(e) as being anticipated by Kocher, et al. (US 6,304,658).

As per claim 1:

Kocher, et al. discloses a method for protecting an electronic system implementing a cryptographic process involving calculation of a modular exponentiation of a quantity (x) **[col.12, lines 56-60]**, said modular exponentiation using a secret exponent (d), comprising breaking down said secret exponent (d) into a plurality of k unpredictable values (dl, d2, ..., dk) **[col.6, lines 50-53]**, the sum of which is equal to said secret exponent. **[col.16, lines 44-45]**

As per claim 2:

Kocher discusses a method according to claim 1 , characterized in that said unpredictable values (d1, d2, ..., dk), are obtained by:

a) deriving (k-1) values by means of a random generator, and **[col.6, lines 50-53]**

b) taking the difference between the secret exponent and the (k-1) values to derive a final value. **[col.8, lines 15-16; col.16, lines 36-40]**

As per claim 3:

Kocher discusses method according to claim 1 , wherein calculation of the modular exponentiation is performed by:

a) raising the quantity (x) by an exponent comprising said value to obtain a set of results for each of said k values; and **[col.5, lines 55-57]**

b) calculating a product of the results obtained in step a). **[col.16, lines 46-50]**

As per claim 4:

Kocher discusses method according to claim 1, wherein at least one of said (k-1) values is obtained by means of a random generator and has a length at least equal to 64 bits. **[col.4, lines 58-60]**

As per claim 5:

Kocher discusses utilizing the method according to claim 1 in a smart card comprising information processing means. **[col.21, line 25]**

As per claim 6:

Kocher discusses utilizing the method according to claim 1 for protecting a cryptographic calculation process using the RSA algorithm. **[col.15, lines 22-27]**

As per claim 7:

Kocher discusses utilizing the method according to claim 1 for protecting a cryptographic calculation process using the Rabin algorithm. **[col.10, lines 28-31 and col.12, lines 18-21]**

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

*****TC 2100 will be moved to Carlyle in October 2004. At this time, any inquiry or communications should be directed to the examiner, LEYNNA HA, whose new telephone number is (571) 272-3851 and the new telephone number for TC 2100 receptionist is 571-272-2100.**

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER